Attorney Docket No. **09792909-6437** (formerly 09798423-0006) PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Patent Application of:

Akira Nonaka, et al.

Application No. **09/856,276**

Filed: **October 2, 2001**

For: DATA PROVIDING SYSTEM AND METHOD THEREFOR

Group Art Unit: **2161**

Examiner: **Frantz Coby**

I hereby certify that this document is being deposited with the United States Postal Service as first class mail in an envelope addressed to: MAIL STOP Appeal Brief - Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on April 21, 2006.

Antonietta Musto

MAIL STOP APPEAL BRIEF - PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF APPELLANTS' APPEAL BRIEF

Enclosed is Appellants' Appeal Brief for the above-referenced United States Patent Application, and a credit card payment form in the amount of $500.00 for filing the Appeal Brief. Appellants believe that the Brief is in full compliance with 37 C.F.R. § 41.37.

The Commissioner is hereby authorized to charge the extension fee and any additional fees which may be required, or to credit any overpayment to Account No. 19-3140. **A duplicate of this sheet is enclosed.**

Respectfully submitted,

Dated: April 21, 2006

By: _____

Marina N. Saito
Registration No. 42,121
SONNENSCHEIN NATH & ROSENTHAL LLP
P.O. Box 061080
Wacker Drive Station, Sears Tower
Chicago, Illinois 60606-1080
(312) 876-8000

Attorney Docket No. **09792909-6437** (formerly 09798423-0006) PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Patent Application of:

Akira Nonaka, et al.

Application No. **09/856,276**

Filed: **October 2, 2001**

For: DATA PROVIDING SYSTEM AND METHOD THEREFOR

Group Art Unit: **2161**

Examiner: **Frantz Coby**

I hereby certify that this document is being deposited with the United States Postal Service as first class mail in an envelope addressed to: MAIL STOP Appeal Brief Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on April 21, 2006.

Antonietta Musto

MAIL STOP APPEAL BRIEF - PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPELLANTS' BRIEF ON APPEAL

Dear Sir:

In accordance with the provisions of 37 C.F.R. § 41.37, Appellants herewith submit this Brief in support of the Appeal for the above-referenced application.

I. REAL PARTY IN INTEREST

The real party in interest in the present appeal is the Assignee, Sony Corporation, a Japanese Corporation. The Assignment was recorded in the U.S. Patent and Trademark Office at Reel 012223, Frame 0442.

II. RELATED APPEALS AND INTERFERENCES

There are no related appeals and no related interferences.

III. STATUS OF CLAIMS

Claims 1-5, 71, 140, 141, 287 and 288 are pending in this application. Claims 6-70, 72-139 and 142-286 have been cancelled. The present Appeal is directed to claims 1-4, 71, 140, and 287-288 that were rejected under 35 U.S.C. § 102(b) as being anticipated by Linehan et al. (U.S. Patent No. 5,495,533), and claims 5 and 141 that were rejected under 35 U.S.C. § 103(a) as being unpatentable over Linehan et al. (U.S. Patent No. 5,495,533) in view of Kravitz et al. (U.S. Patent No. 6,738,905) in a final office action dated September 23, 2005.

IV. STATUS OF AMENDMENTS

There are no pending amendments. However, appellants reserve the right to submit an amendment to correct noted typographical errors that do not affect the appeal.

V. SUMMARY OF CLAIMED SUBJECT MATTER

The present invention is directed to a data providing system for distributing content data from a data providing apparatus to a data processing apparatus and managing the data providing apparatus and the data processing apparatus by a management apparatus. (See page 75, line 1 through page 79, line 20.) The management apparatus prepares a key file storing encrypted content key data and encrypted usage control policy data indicating a content of rights such as usage permission conditions of the content data. (See page 87, lines 8-14 and page 75, lines 13-19.) The data providing apparatus receives the key file storing encrypted content key data and encrypted usage control policy data, and distributes a module storing a content file storing the content data encrypted by using the content key data and the key file received from the

management apparatus to the data processing apparatus. (See page 107, line 15 through page 108, line 11.) The data processing apparatus receives the module containing the key file, decrypts the content key data and the usage control policy data stored in the key file, and determines the handling of the content data based on the decrypted usage control policy data. (See page 123, line 18 through page 127, line 14.) In particular, the data processing apparatus determines at least one between a purchase form and a usage form of the content data based on the usage control policy data, and transmits a log data indicating the log of the determined at least one of the related purchase form and usage form to the management apparatus. (See page 127, line 12 through page 130, line 13.)

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

1. Claims 1-4, 71, 140, and 287-288 stand rejected under 35 U.S.C. § 102(b) as anticipated by Linehan et al. (U.S. Patent No. 5,495,533).

2. Claims 5 and 141 stand rejected under 35 U.S.C. § 103(a) as obvious over Linehan et al. in view of Kravitz et al. (U.S. Patent No. 6,738,905).

VII. ARGUMENT

Claims 1-4, 71, 140, and 287-288 are patentable over Linehan et al., and claims 5 and 141 are patentable over Linehan et al. in view of Kravitz et al.

A. The Claimed Invention

Claim 1 is directed to a data providing system for distributing content data from a data providing apparatus to a data processing apparatus and managing the data providing apparatus

and the data processing apparatus by a management apparatus. The management apparatus prepares a key file storing encrypted content key data and encrypted usage control policy data indicating a content of rights such as usage permission conditions of the content data. The data providing apparatus provides the content data encrypted by using the content key data. The data processing apparatus decrypts the content key data and the usage control policy data stored in the key file and determines the handling of the content data based on the decrypted usage control policy data.

Claims 2-5 depend from claim 1.

Claim 71 is directed to a data providing method for distributing content data from a data providing apparatus to a data processing apparatus and managing the data providing apparatus and the data processing apparatus by a management apparatus. The management apparatus prepares a key file storing encrypted content key data and encrypted usage control policy data indicating a content of rights such as usage permission conditions of the content data. The data providing apparatus provides the content data encrypted by using the content key data. The data processing apparatus decrypts the content key data and the usage control policy data stored in the key file and determines the handling of the content data based on the related decrypted usage control policy data.

Claim 140 is directed to a data providing apparatus which is managed by a management apparatus and distributes content data to a data processing apparatus receiving a key file storing encrypted content key data and encrypted usage control policy data indicating a content of rights such as usage permission conditions of said content data, and distributing a module storing a

content file storing the content data encrypted by using said content key data and said key file received from said management apparatus to said data processing apparatus.

Claim 141 is directed to a data processing apparatus managed by a management apparatus and utilizing content data, receiving a module containing a key file storing encrypted content key data and encrypted usage control policy data indicating a content of rights such as usage permission conditions of said content data and a content file storing the content data encrypted by using said content key data, determining at least one between a purchase form and an usage form of said content data based on said usage control policy data, and transmitting a log data indicating the log of the determined at least one of the related purchase form and usage form to said management apparatus.

Claim 287 is directed to a data providing method which is managed by a management apparatus and distributes content data to a data processing apparatus, receiving a key file storing encrypted content key data and encrypted usage control policy data indicating a content of rights such as usage permission conditions of said content data, and distributing a module storing a content file storing the content data encrypted by using said content key data and said key file received from said management apparatus to said data processing apparatus.

Claim 288 is directed to a data processing method managed by a management apparatus and utilizing content data, receiving a module containing a key file storing encrypted content key data and encrypted usage control policy data indicating a content of rights such as usage permission conditions of said content data and a content file storing the content data encrypted by using said content key data, determining at least one between a purchase form and an usage form of said content data based on said usage control policy data, and transmitting a log data

indicating the log of the determined at least one of the related purchase form and usage form to said management apparatus.

B. Claims 1-4, 71, 140 And 287-288 Are Patentable

In the Final Office Action, claims 1-4, 71, 140, and 287-288 were rejected under 35 U.S.C. § 102(b) as being anticipated by Linehan et al. (U.S. Patent No. 5,495,533), and claims 5 and 141 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Linehan et al. (U.S. Patent No. 5,495,533) in view of Kravitz et al. (U.S. Patent No. 6,738,905). The Examiner has not made an adequate showing to support his rejections.

Linehan et al. is directed to a security system that automatically manages keys used for encryption or message authentication of data files or individual entries in databases. (See col. 6, lines 8-10.) The personal key archive security system uses two components: the Personal Key Client component on a user computer and the Personal Key Server. (See col. 6, lines 17-20.) The Personal Key Server maintains a Personal Key Database that contains certain information required to decrypt files or check their message authentication. (See col. 7, lines 6-9.)

In Linehan et al., each data file is encrypted by the Personal Key Client at the time the file is created. (See col. 7, lines 30-33.) The Personal Key Server Database contains an entry for each file that is encrypted, and each entry contains the key used to encrypt the corresponding file, the name of the owner of the file, and the access control list containing the names of any of the users who are permitted to access the file. (See col. 7, lines 39-45.) In Linehan et al., the access control list is not encrypted. Thus, Linehan et al. neither discloses nor suggests that the management apparatus prepares a key file storing encrypted usage control policy data indicating a content of rights such as usage permission conditions of the content data, or that the data

processing apparatus decrypts the usage control policy data stored in the key file and determines the handling of the content data based on the decrypted usage control policy data, as required by the claims.

In the Advisory Action, the Examiner stated that

> Linehan provides an automated management system for managing keys to encrypt and decrypt stored data on the computing system. In addition, Linehan provides a mechanism showing the organization of file headers used with key archives that primarily incorporates an access control list (See Linehan et al. Figure 8). The access control list primarily indicates content of rights including usage permission conditions of content data because the access control list includes list of users permitted to access the file (See Linehan et al. Col. 8, lines 57-65).

The Examiner does not appear to dispute that the usage control policy data in Linehan et al. is not encrypted before it is stored in the key file.

Moreover, in Linehan et al., when a file is created, the Personal Key Client sends the ticket of the creator, along with the file's name and creation date, to the Personal Key Server. (See col. 7, lines 47-49.) The Personal Key Server generates a file encryption key, creates a new entry in the database, and responds to the Personal Key Client with the file encryption key. (See col. 7, lines 49-52.) The Personal Key Client then uses the key to encrypt the data as it is written to the file. (See col. 7, lines 52-53.)

When a file is accessed, the Personal Key Client sends the ticket of the accessor, the file's name, and the file's creation date to the Personal Key Server. (See col. 7, lines 54-57.) The Personal Key Server retrieves the appropriate entry in the database and checks the identity of the accessor as provided in the ticket against the file owner's name and access control list in the database entry. (See col. 7, lines 57-60.) If the accessor is either the owner or one of the users named in the access control list, the Server sends the file encryption key back to the Personal

Key Client. (See col. 7, lines 60-63.) The Personal Key Client uses the key to decrypt the data as it is read from the file. (See col. 7, lines 63-64.) Thus, in Linehan et al., the Personal Key Server that generates the file encryption key and maintains the Personal Key Server Database does not store the encrypted file. Accordingly, Linehan et al. does not disclose or suggest a management apparatus that prepares a key file storing encrypted content key data and encrypted usage control policy data indicating a content of rights such as usage permission conditions of said content data, as required by the claims. The Examiner does not appear to dispute this fact.

In view of the foregoing, Appellants respectfully submit that claims 1-4, 71, 140, 287 and 288 are patentable and the application is in condition for allowance.

C. Claims 5 and 141 Are Patentable

As discussed above, Linehan et al. does not disclose or suggest various limitations that are required by the claims. Thus, it would not have been obvious to one skilled in the art at the time of the invention to modify Linehan et al. with the disclosure of Kravitz et al. to derive claim 5 or claim 141, both of which include these limitations.

In view of the foregoing, Appellants respectfully submit that claims 5 and 141 are patentable and the application is in condition for allowance.

D. Conclusion

Appellants respectfully submit that the subject matter of the claims on appeal is not disclosed or suggested by Linehan et al. Thus, the Examiner has not made an adequate showing of anticipation with respect to the subject matter of the rejected claims. Appellants, therefore, respectfully request reversal of the Examiner's decision to reject claims 1-4. 71, 140 and 287-288

under 35 U.S.C. § 102(b) over Linehan et al., and claims 14 and 25 under 35 U.S.C. § 103(a) as being unpatentable over Linehan et al. in view of Misra, and respectfully request allowance of all pending claims.

Respectfully submitted,

Dated: April 21, 2006

By: _____

Marina N. Saito
Registration No. 42,121
SONNENSCHEIN NATH & ROSENTHAL LLP
P.O. Box 061080
Wacker Drive Station, Sears Tower
Chicago, Illinois 60606-1080
(312) 876-8000

VIII. CLAIMS APPENDIX

1. (Previously Presented) A data providing system for distributing content data from a data providing apparatus to a data processing apparatus and managing said data providing apparatus and said data processing apparatus by a management apparatus, wherein

said management apparatus prepares a key file storing encrypted content key data and encrypted usage control policy data indicating a content of rights such as usage permission conditions of said content data,

said data providing apparatus provides said content data encrypted by using said content key data, and

said data processing apparatus decrypts said content key data and said usage control policy data stored in said key file and determines the handling of said content data based on the decrypted usage control policy data.

2. (Previously Presented) A data providing system as set forth in claim 1, wherein said management apparatus adds signature data for verification to the key file.

3. (Original) A data providing system as set forth in claim 1, wherein said data providing apparatus prepares a content file storing the content data and provides the content file to the data processing apparatus.

4. (Previously Presented) A data providing system as set forth in claim 3, wherein said data providing apparatus adds signature data for verification to the content file.

5. (Original) A data providing system as set forth in claim 1, wherein

the data providing apparatus prepares usage control policy data and sends it to said management apparatus,

said data processing apparatus determines at least one of the purchase form and the usage form of the distributed content data based on the usage control policy data and sends log data showing the log of at least one of the purchase form and the usage form decided to said management apparatus, and

said management apparatus performs profit distribution processing for distributing the profit obtained along with the purchase and usage of the content data in the data processing apparatus to the interested parties of the data providing apparatus based on the received log data.

6-70. (Cancelled).

71. (Previously Presented) A data providing method for distributing content data from a data providing apparatus to a data processing apparatus and managing said data providing apparatus and said data processing apparatus by a management apparatus, wherein

said management apparatus prepares a key file storing encrypted content key data and encrypted usage control policy data indicating a content of rights such as usage permission conditions of said content data,

said data providing apparatus provides said content data encrypted by using said content key data, and

said data processing apparatus decrypts said content key data and said usage control policy data stored in said key file and determines the handling of said content data based on the related decrypted usage control policy data.

72-139. (Cancelled).

140. (Previously Presented) A data providing apparatus which is managed by a management apparatus and distributes content data to a data processing apparatus,

receiving a key file storing encrypted content key data and encrypted usage control policy data indicating a content of rights such as usage permission conditions of said content data, and

distributing a module storing a content file storing the content data encrypted by using said content key data and said key file received from said management apparatus to said data processing apparatus.

141. (Previously Presented) A data processing apparatus managed by a management apparatus and utilizing content data,

receiving a module containing a key file storing encrypted content key data and encrypted usage control policy data indicating a content of rights such as usage permission conditions of said content data and a content file storing the content data encrypted by using said content key data,

determining at least one between a purchase form and an usage form of said content data based on said usage control policy data, and

transmitting a log data indicating the log of the determined at least one of the related purchase form and usage form to said management apparatus.

142-286. (Cancelled).

287. (Previously Presented) A data providing method which is managed by a management apparatus and distributes content data to a data processing apparatus,

receiving a key file storing encrypted content key data and encrypted usage control policy data indicating a content of rights such as usage permission conditions of said content data, and

distributing a module storing a content file storing the content data encrypted by using said content key data and said key file received from said management apparatus to said data processing apparatus.

288. (Previously Presented) A data processing method managed by a management apparatus and utilizing content data,

receiving a module containing a key file storing encrypted content key data and encrypted usage control policy data indicating a content of rights such as usage permission conditions of said content data and a content file storing the content data encrypted by using said content key data,

determining at least one between a purchase form and an usage form of said content data based on said usage control policy data, and

transmitting a log data indicating the log of the determined at least one of the related purchase form and usage form to said management apparatus.

X. EVIDENCE APPENDIX

Appellants attach hereto copies of the patents to (1) Linehan et al. (U.S. Patent No. 5,495,533), and (2) Kravitz et al. (U.S. Patent No. 6,738,905) , which were relied upon by the Examiner in his rejection entered on February 16, 2005.

IX. RELATED PROCEEDINGS APPENDIX

There are no related proceedings.